PRESENT

An Ultra-Lightweight Block Cipher

A. Bogdanov\textsuperscript{1}, L. R. Knudsen\textsuperscript{3}, G. Leander\textsuperscript{1}, C. Paar\textsuperscript{1}, A. Poschmann\textsuperscript{1}, M. J. B. Robshaw\textsuperscript{2}, Y. Seurin\textsuperscript{2}, C. Vikkelsoe\textsuperscript{3}

1 Ruhr-Universität Bochum
2 Technical University Denmark, Denmark
3 Orange Lab, France

CHES 2007
Outline

- Motivation
- PRESENT Specification
- Security Analysis
- Implementation Results
- Conclusion
Why yet another Block Cipher? (1)

• Paradigm shift towards Pervasive Computing:
  • cost driven deployment
  • very constrained devices in terms of CPU, memory, power, and energy
  • small messages
• Traditionally efficient equivalent to high throughput
  • Known ciphers designed for high throughput, high speed, high …

Demand for an ultra-lightweight block cipher
Why yet another Block Cipher? (2)

• Security properties well understood
• Sound building blocks and design principles available
• Block ciphers can be used
  • as stream ciphers
  • for hashing
Metric and Tradeoffs

Resistance against attacks

256 bits

48 rounds

16 rounds

80 bits

Security

Low Cost

Performance

Area, Power

serial

parallel

Throughput, Energy

Parallelism
Requirements on PRESENT

• Design goals
  • Efficient hardware implementations
  • Moderate security level (80 bits)
  • Simplicity
• Small amounts of plaintexts
• encryption only core
• Metrics:
  1. Security
  2. Area, Power
  3. Speed
Outline

- Motivation
- PRESENT Specification
- Security Analysis
- Implementation Results
- Conclusion
generateRoundKeys()

for $i = 1$ to $31$ do
    addRoundKey($\text{STATE}, K_i$)
    sBoxLayer($\text{STATE}$)
    pLayer($\text{STATE}$)
end for

addRoundKey($\text{STATE}, K_{32}$)
S-Boxes in Hardware

- LUT are realized as boolean functions
- Highly non-linear
- High boolean complexity
- Big area

- AES-LUT 1000
- AES-CF 300
- DES 120
- PRESENT 28
S-Box Design Criteria

We denote the Fourier coefficient of $S$ by

$$S_b^W(a) = \sum_{x \in \mathbb{F}_2^4} (-1)^{\langle b, S(x) \rangle + \langle a, x \rangle}.$$ 

1. For any fixed non-zero input difference $\Delta_i \in \mathbb{F}_2^4$ and any fixed non-zero output difference $\Delta_o \in \mathbb{F}_2^4$ we require

$$\# \{x \in \mathbb{F}_2^4 | S(x) + S(x + \Delta_i) = \Delta_o \} \leq 4.$$ 

2. For any fixed non-zero input difference $\Delta_i \in \mathbb{F}_2^4$ and any fixed output difference $\Delta_o \in \mathbb{F}_2^4$ such that $\text{wt}(\Delta_i) = \text{wt}(\Delta_o) = 1$ we have

$$\{x \in \mathbb{F}_2^4 | S(x) + S(x + \Delta_i) = \Delta_o \} = \emptyset.$$ 

3. For all non-zero $a \in \mathbb{F}_2^4$ and all non-zero $b \in \mathbb{F}_4$ it holds that $|S_b^W(a)| \leq 8$. 

4. For all $a \in \mathbb{F}_2^4$ and all non-zero $b \in \mathbb{F}_4$ such that $\text{wt}(a) = \text{wt}(b) = 1$ it holds that $S_b^W(a) = \pm 4$. 
PRESENT S-Box

<table>
<thead>
<tr>
<th>x</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>S[x]</td>
<td>C</td>
<td>5</td>
<td>6</td>
<td>B</td>
<td>9</td>
<td>0</td>
<td>A</td>
<td>D</td>
<td>3</td>
<td>E</td>
<td>F</td>
<td>8</td>
<td>4</td>
<td>7</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

• Smallest 4x4 S-Boxes in hardware (28 GE)
• Fullfilling above conditions
### PRESENT Permutation

<table>
<thead>
<tr>
<th>$i$</th>
<th>$P(i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>32</td>
</tr>
<tr>
<td>3</td>
<td>48</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td>6</td>
<td>33</td>
</tr>
<tr>
<td>7</td>
<td>49</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>34</td>
</tr>
<tr>
<td>11</td>
<td>50</td>
</tr>
<tr>
<td>12</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>19</td>
</tr>
<tr>
<td>14</td>
<td>35</td>
</tr>
<tr>
<td>15</td>
<td>51</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$i$</th>
<th>$P(i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td>17</td>
<td>20</td>
</tr>
<tr>
<td>18</td>
<td>36</td>
</tr>
<tr>
<td>19</td>
<td>52</td>
</tr>
<tr>
<td>20</td>
<td>5</td>
</tr>
<tr>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>22</td>
<td>37</td>
</tr>
<tr>
<td>23</td>
<td>53</td>
</tr>
<tr>
<td>24</td>
<td>6</td>
</tr>
<tr>
<td>25</td>
<td>22</td>
</tr>
<tr>
<td>26</td>
<td>38</td>
</tr>
<tr>
<td>27</td>
<td>54</td>
</tr>
<tr>
<td>28</td>
<td>7</td>
</tr>
<tr>
<td>29</td>
<td>23</td>
</tr>
<tr>
<td>30</td>
<td>39</td>
</tr>
<tr>
<td>31</td>
<td>55</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$i$</th>
<th>$P(i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>8</td>
</tr>
<tr>
<td>33</td>
<td>24</td>
</tr>
<tr>
<td>34</td>
<td>40</td>
</tr>
<tr>
<td>35</td>
<td>56</td>
</tr>
<tr>
<td>36</td>
<td>9</td>
</tr>
<tr>
<td>37</td>
<td>25</td>
</tr>
<tr>
<td>38</td>
<td>41</td>
</tr>
<tr>
<td>39</td>
<td>57</td>
</tr>
<tr>
<td>40</td>
<td>10</td>
</tr>
<tr>
<td>41</td>
<td>26</td>
</tr>
<tr>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>43</td>
<td>58</td>
</tr>
<tr>
<td>44</td>
<td>11</td>
</tr>
<tr>
<td>45</td>
<td>27</td>
</tr>
<tr>
<td>46</td>
<td>43</td>
</tr>
<tr>
<td>47</td>
<td>59</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$i$</th>
<th>$P(i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>12</td>
</tr>
<tr>
<td>49</td>
<td>28</td>
</tr>
<tr>
<td>50</td>
<td>44</td>
</tr>
<tr>
<td>51</td>
<td>60</td>
</tr>
<tr>
<td>52</td>
<td>13</td>
</tr>
<tr>
<td>53</td>
<td>29</td>
</tr>
<tr>
<td>54</td>
<td>45</td>
</tr>
<tr>
<td>55</td>
<td>61</td>
</tr>
<tr>
<td>56</td>
<td>14</td>
</tr>
<tr>
<td>57</td>
<td>30</td>
</tr>
<tr>
<td>58</td>
<td>46</td>
</tr>
<tr>
<td>59</td>
<td>62</td>
</tr>
<tr>
<td>60</td>
<td>15</td>
</tr>
<tr>
<td>61</td>
<td>31</td>
</tr>
<tr>
<td>62</td>
<td>47</td>
</tr>
<tr>
<td>63</td>
<td>63</td>
</tr>
</tbody>
</table>

- Simple bit permutation
PRESENT Permutation - in Hardware

- Just wires
- No transistors required
- No delay

0 GE
(some wiring)
PRESENT Key Schedule

Notation:

- $K$ 80-bit key register
- At round 1: $K = k_{79}k_{78}...k_1k_0 = $ initial key
- At round $i$: $K_i = k_{79}k_{78}...k_1k_{16} = $ roundkey for round $i$

Updating $K$:

2. $[k_{79}k_{78}...k_1k_0] = [k_{18}k_{17}...k_{20}k_{19}]$

3. $[k_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$

4. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15}] \text{ XOR round\_counter}$
Outline

- Motivation
- PRESENT Specification
- Security Analysis
- Implementation Results
- Conclusion
Differential Cryptanalysis

Theorem 1:

Any 5-round differential characteristic of PRESENT has at least 10 active S-Boxes.

• Any differential characteristic over 25 rounds must have at least 50 active S-Boxes

• Maximum differential characteristic is $2^{-2}$

• Probability of 25-round characteristic is bounded by

\[
(2^{-2})^{50} = 2^{-100}
\]

\[
2^{100} >> 2^{64} \text{ (available PT/CT pairs)}
\]

\[
2^{100} >> 2^{80} \text{ (key size)}
\]
Linear Cryptanalysis

Theorem 2:
Let $\varepsilon_{4R}$ be the maximal bias of a linear approximation of four rounds of PRESENT. Then $\varepsilon_{4R} \leq 2^{-7}$.

- The maximum bias of a 28-round linear approximation is $2^6 \times (\varepsilon_{4R})^7 = 2^6 \times (2^{-7}) = 2^{-43}$
- About $(2^{43})^2 = 2^{86}$ known PT/CT pairs required

$2^{86} >> 2^{64}$ (available plaintext)
$2^{86} >> 2^{80}$ (key size)
Algebraic Cryptanalysis

- The PRESENT 4 x 4 S-Boxes can be described by 21 equations over GF(2) using 8 variables
  - $21 \times 17 \times 31 = 11,067$ quadratic equations
  - $8 \times 17 \times 31 = 4,216$ variables

- Small scale version analyzed
  - 7 S-Boxes
  - 28 bit block
  - 2 rounds

Buchberger and $F_4$ algorithm fail to deliver a solution in a reasonable time for this 2-round 28-bit mini-PRESENT
Outline

- Motivation
- PRESENT Specification
- Security Analysis
- Implementation Results
- Conclusion
Toolchain

Mentor Graphics ModelSim SE Plus 5.8c

Synopsys DesignCompiler Y-2006-06

Virtual Silicon UMCL18G212T3
PRESENT-80 Datapath

- plaintext
  - 1.8 V
  - 25°C

- ciphertext
  - 32 cycles
  - 1570 GE
  - 5 µW@100kHz
Comparison of Lightweight Ciphers

- CLEFIA: 4993
- AES: 3400
- HIGHT: 3048
- DESXL: 2168
- PRESENT-128: 1886
- PRESENT-80: 1570
- TRIVIUM: 2599
- GRAIN: 1294
Outline

- Motivation
- PRESENT Specification
- Security Analysis
- Implementation Results
- Conclusion
Conclusion

• Presented the new block cipher PRESENT
• SPN with 64-bit state, 80-bit key, 31 rounds
• Based on well-known design principles (feature)
• Very small footprint in hardware (1570 GE)
• Low power estimates (5 µW)
• Lightweight block ciphers have similar footprint as stream ciphers

Please try to break PRESENT!
Thank you!

Questions?

www.crypto.rub.de
poschmann@crypto.rub.de
PRESENT Permutation - Further Notes

\[
P(i) = \begin{cases} 
16 \times i \mod 63, & 1 \leq i \leq 62 \\
i, & i \in \{0,63\}
\end{cases}
\]

- Involution $P(P(P(i))) = i$
- Could be useful for serialization